INEEL/EXT-05-02649

Power Systems Control Architecture

James R. Davidson

January 2005

Idaho National Engineering and Environmental Laboratory
Bechtel BWXT Idaho, LLC

INEEL/EXT-05-02649

Power Systems Control Architecture

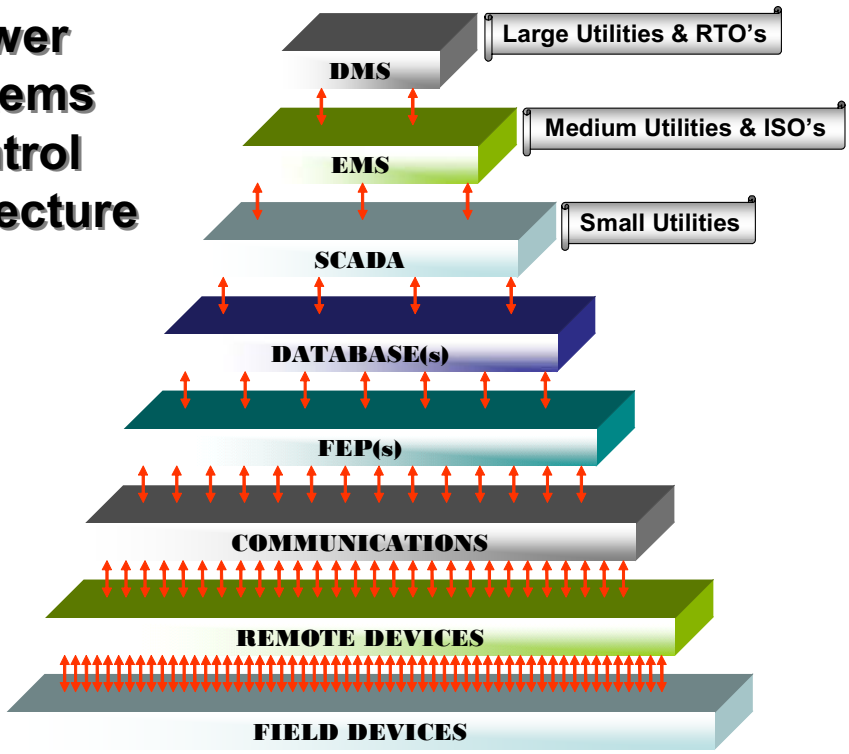
James R. Davidson

January 2005

Idaho National Engineering and Environmental Laboratory
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy, Science and Technology
Under DOE Idaho Operations Office
Contract DE-AC07-99ID13727

Power Systems Control Architecture



Introduction

The diagram above depicts the complexity of the power systems control architecture used by the national power structure. It shows the structural hierarchy and the relationship of the each system to those other systems interconnected to it.

Each of these levels provides a different focus for vulnerability testing and has its own weaknesses. In evaluating each level, of prime concern is what vulnerabilities exist that provide a path into the system, either to cause the system to malfunction or to take control of a field device.

An additional vulnerability to consider is can the system be compromised in such a manner that the attacker can obtain critical information about the system and the portion of the national power structure that it controls.

DMS – Distributed Management Systems normally communicate with multiple EMS's via TASE.2 (ICCP) communications channels and provide an overview monitoring system. When used in the Regional Transmission Organizations (RTO's) they rarely provide control functions.

EMS – Energy Management Systems provide higher level functions to SCADA systems such as power projections, Automatic Generator Controls (AGC), forecasting, load balancing, etc. In the case of Independent System Operators (ISO's) these systems typically communicate with multiple SCADA systems via TASE.2 (ICCP) communications channels and rarely provide any control functions. EMS can communicate with a single or multiple SCADA systems.

SCADA – Supervisory Control and Data Acquisition systems are the heart of the control portions of a Power System. They drive the various components that acquire and process information from field devices.

Databases – There are three main types of databases used in these systems. The real time database is used to store data coming from the Front End Processors. The relational database, if used, provides better access to the information in the real-time database. Finally, the historical database provides a historical record of the operation of the SCADA system along with pertinent data.

FEP - Front End Processors provide communications with the field devices, identifying the protocols, physical communications methods, interpreter, and acts as an interface between the databases and the actual communications.

Communications – This is the portion that provides the electronic links between the SCADA system and the field devices. Communications can be via networking, modem, wireless, radio, satellite, microwave, and other communications systems.

Remote Devices – These are the devices that obtain the raw data from the field signals, process the signals, and communication the values or states of these signals to the SCADA system. They provide not only a method to monitor, but also control functions to the various devices used in the electrical system. These include: Remote Terminal Units (RTU's), Programmable Logic Controllers (PLC's), Intelligent Electronic Devices (IED's) as well as connectivity to substation automation systems.

Field Devices – These are the devices that provide the real data and control functions. They can be sensors (Voltage, Current, VAR, etc.), controls (Relays, Breakers, Generators, etc.), or status monitoring devices.